(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
26. Juli 2001 (26.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/54083 A1

(51) Internationale Patentklassifikation[7]: G07F 7/10, G11C 7/24

(21) Internationales Aktenzeichen: PCT/DE00/04448

(22) Internationales Anmeldedatum:
14. Dezember 2000 (14.12.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
00100955.4 18. Januar 2000 (18.01.2000) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Strasse 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **GAMMEL, Berndt** [DE/DE]; Ludwig-Dill-Weg 3, 81737 München (DE). **KNIFFLER, Oliver** [DE/DE]; Weddigenstrasse 1, 81737 München (DE). **SEDLAK, Holger** [DE/DE]; Neumünster 10 a, 85658 Egmating (DE).

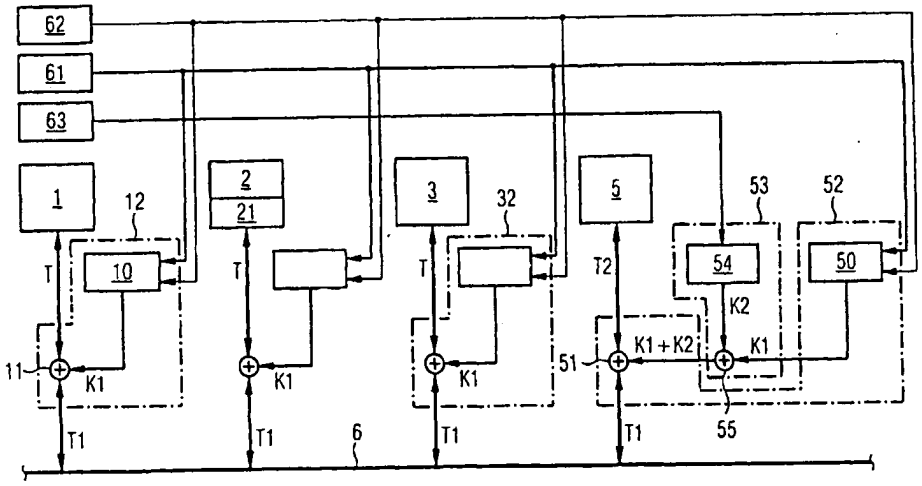
(74) Anwalt: **EPPING HERMANN & FISCHER GBR**; Postfach 12 10 26, 80034 München (DE).

(81) Bestimmungsstaaten *(national)*: BR, CN, IN, JP, KR, MX, RU, UA, US.

[Fortsetzung auf der nächsten Seite]

(54) Title: MICROPROCESSOR SYSTEM WITH ENCODING

(54) Bezeichnung: MIKROPROZESSORANORDNUNG MIT VERSCHLÜSSELUNG



(57) **Abstract:** A microcontroller for security applications, comprising an encoding unit (12, 32, 52) between a bus (6) and a functional unit (1, 2, 3, 5) which include a gate (11, 51) and a key register (10, 50) Another encoding unit (53) is provided in a memory (5). The gate (51) of said encoding unit is mounted between the register (50) and the gate (51) of the first encoding unit (52). As a result, information transmitted is encoded at each point on the bus (6).

(57) **Zusammenfassung:** Ein Mikrocontroller für Sicherheitsanwendungen umfaßt eine Verschlüsselungseinheit (12, 32, 52) zwischen einem Bus (6) und einer Funktionseinheit (1, 2, 3, 5), die ein Gatter (11, 51) und ein Schlüsselregister (10, 50) umfassen. Bei einem Speicher (5) ist eine weitere Verschlüsselungseinheit (53) vorgesehen, deren Gatter (55) zwischen das Register (50) und das Gatter (51) der ersten Verschlüsselungseinheit (52) geschaltet ist. Dadurch wird erreicht, daß an jeder Stelle des Busses (6) die übertragene Information verschlüsselt vorliegt.

WO 01/54083 A1

(84) **Bestimmungsstaaten** *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Mikroprozessoranordnung mit Verschlüsselung

Die Erfindung betrifft eine Mikroprozessoranordnung, bei der eine zentrale Verarbeitungseinheit, eine weitere Einheit sowie eine Speichereinheit über einen Bus miteinander verbunden sind und eine Verschlüsselung durchgeführt wird.

Solche Mikroprozessoranordnungen werden in sicherheitskritischen Anwendungen eingesetzt, beispielsweise in einer Chipkarte. Die Anordnung ist auf einem einzigen Halbleiterchip integriert, sogenannter Mikrocontroller. Über den Bus wird sämtlicher Datenverkehr abgewickelt. Der Bus übermittelt beispielsweise Daten, Adressen, Programmbefehle, Steuerbefehle etc. Die abzuarbeitenden Programme sind in einem nichtflüchtigen Speicher (ROM) gespeichert, Daten können ebenfalls im nichtflüchtigen Speicher oder temporär in einem flüchtigen Speicher (RAM) gespeichert werden. Wegen der langen Zugriffszeit auf diese Speicher werden die zu verarbeitenden Daten in schnelleren Cache-Speichern zwischengepuffert.

Sämtliche Speicher sowie die Busse auf dem Mikroprozessor oder Mikrocontroller sind leicht zu identifizierende regelmäßige Strukturen auf dem Chip. Sie stellen daher bevorzugte Angriffspunkte dar, wenn versucht wird, chipinterne Schaltungen oder Betriebsabläufe abzugreifen, um sicherheitsrelevante Daten und Funktionen auszuspähen. Etwaige Angriffe können durch Probing erfolgen, bei dem durch Aufsetzen von Nadeln auf interessierende Strukturen die Signalverläufe abgegriffen werden.

Im Speicher abgelegte Daten sind daher bei herkömmlichen Mikroprozessoren oder -controllern mit einer aufwendigen Verschlüsselung chiffriert. Das Auslesen erfordert entsprechenden Rechenaufwand. Die anschließende Übertragung der Daten und Einspeisung in die verschiedenen Funktionseinheiten des

Mikroprozessors erfolgt in der Regel unverschlüsselt. Bei einem Nadelangriff auf den Bus könnten daher jegliche Daten im Klartext abgefragt werden. Eine vergleichsweise aufwendige Ver- und Entschlüsselung auch des Datenverkehrs von und zur zentralen Verarbeitungseinheit (CPU), einer Peripherieeinheit oder einer arithmetisch-logischen Einheit (ALU) oder des Cache-Speichers empfiehlt sich nicht, da die Zugriffsgeschwindigkeit auf diese Einheiten dadurch wesentlich verringert würde.

Die Aufgabe der Erfindung besteht darin, eine Mikroprozessoranordnung anzugeben, die gegenüber einem Ausspähen von internen Abläufen höhere Sicherheit aufweist.

Gelöst wird diese Aufgabe durch eine Mikroprozessoranordnung, die umfaßt: eine zentrale Verarbeitungseinheit; eine weitere Einheit; eine Speichereinheit; einen Bus, über den die zentrale Verarbeitungseinheit, die weitere Einheit und der Speicher miteinander zum Austausch von Daten verbunden sind; je eine den Einheiten zugeordnete erste Verschlüsselungseinheit, die zwischen den Bus und der zugeordneten Einheit geschaltet ist und ein Mittel zur Bereitstellung eines Schlüssels und ein logisches Verknüpfungselement umfaßt, das zwischen den Bus und die zugeordnete Einheit geschaltet ist, wobei der Schlüssel für die Einheiten gleich ist und veränderbar ist; eine der Speichereinheit zugeordnete zweite Verschlüsselungseinheit, die ein Mittel zur Bereitstellung eines weiteren Schlüssels umfaßt sowie ein logisches Verknüpfungselement, das zwischen das Mittel zur Bereitstellung des Schlüssels der zugeordneten ersten Verschlüsselungseinheit und das logische Verknüpfungselement der zugeordneten ersten Verschlüsselungseinheit geschaltet ist.

Bei der Mikroprozessoranordnung gemäß der Erfindung ist bei jeder an den Bus angeschlossenen Funktionseinheit eine Verschlüsselungseinrichtung vorgesehen, die relativ einfach auf-

gebaut ist. Sie umfaßt ein Mittel zur Bereitstellung eines Schlüssels, beispielsweise ein Register, sowie ein Verknüpfungselement, beispielsweise ein Exklusiv-ODER-Gatter. Die Verschlüsselungseinrichtung ist in der Lage, sowohl eine Verschlüsselung des von der Funktionseinheit auf den Bus ausgegebenen Datums durchzuführen als auch eine Entschlüsselung eines zu empfangenden Datums. Die Verschlüsselungseinrichtung ist einfach aufgebaut und führt daher bei der Datenübertragung zu keiner nennenswerten Verzögerung.

Zweckmäßigerweise wird der Schlüssel, welcher im Register abgelegt ist, von Zeit zu Zeit verändert. Die Aktualisierung des Schlüssels erfolgt vorzugsweise mit jedem Betriebstakt. Damit ein von einer Funktionseinheit auf den Bus ausgegebener und verschlüsselter Datenwert von einer anderen Funktionseinheit bei wechselndem Schlüssel wieder entschlüsselt werden kann, müssen die Schlüsselregister jeder Funktionseinheit bei zusammengehörenden Lese- und Schreibvorgängen den gleichen Schlüssel beinhalten. Der Schlüssel wird zweckmäßigerweise hierzu von einem Schlüsselgenerator erzeugt, der taktsynchron an alle Schlüsselregister den gleichen Schlüssel weiterleitet. Vorzugsweise wird der Schlüssel zufallsgesteuert erzeugt. Trotz der einfachen, kaum Verzögerungszeit beanspruchenden Ver- und Entschlüsselung wird durch die zufällige Bereitstellung verschiedener Schlüsselworte ausreichend Sicherheit vor einem Abgriff und Ausspähen des Datenverkehrs geboten.

Um in einem an den Bus angeschlossenen Speicher, beispielsweise einem Cache-Speicher, einem Puffer-Speicher oder einem Translation Lookaside Buffer zu verhindern, daß die Information im Klartext dort abgespeichert ist, ist eine zusätzliche Ver- bzw. Entschlüsselung erforderlich. Hierzu ist eine weitere Verschlüsselungseinheit vorgesehen, die wiederum ein Mittel zur Bereitstellung des Schlüssels, beispielsweise ein weiteres Schlüsselregister, sowie ein logisches Verknüpfungselement, beispielsweise ein Exklusiv-ODER-Gatter umfaßt. We-

sentlich ist, daß das logische Verknüpfungselement der weiteren Verschlüsselungseinheit zwischen das logische Verknüpfungselement der ersten Verschlüsselungseinheit und deren Schlüsselregister angeordnet ist. Dies hat den Vorteil, daß sämtliche Busabschnitte, insbesondere diejenigen zwischen dem logischen Verknüpfungselement der ersten Verschlüsselungseinheit, welches zwischen Bus und Speicher angeordnet ist, und dem Speicher, nur verschlüsselte Daten führen.

Das Schlüsselregister der zweiten Verschlüsselungseinheit wird von einem weiteren Schlüsselgenerator gespeist. Zweckmäßigerweise wird auch dieser Schlüssel von Zeit zu Zeit verändert. Dabei ist zu gewährleisten, daß im Speicher verschlüsselt zwischengespeicherte Daten mit dem gleichen Schlüssel wieder ausgelesen werden. Der Schlüssel für das genannte Schlüsselregister wird daher nur dann aktualisiert, wenn der Speicher keine gültige Information mehr enthält. Dies ist beispielsweise dann der Fall, wenn der Speicher vollständig entleert ist oder wenn der Speicher neu initialisiert wird. Dies erfolgt beispielsweise dann, wenn die Mikroprozessoranordnung eine Anwendung beendet hat und eine neue Anwendung beginnt. Bei einem solchen Applikationswechsel ist es aus Sicherheitsgründen nicht mehr erforderlich, den Speicherinhalt zu ändern, da durch den Schlüsselwechsel der im Speicher noch enthaltene Dateninhalt ohnehin von einer neuen Anwendung nicht mehr verwertbar ist.

In Ausgestaltung der Erfindung umfassen die Verschlüsselungseinheiten nur Exklusiv-ODER-Gatter und zugehörige Schlüsselregister bei jeder an den Bus angeschlossenen Funktionseinheit. Der schaltungstechnische Aufwand ist relativ gering. Die Schlüsselgeneratoren sind jeweils nur in einfacher Ausführung vorzusehen. Der zusätzliche Rechenaufwand ist gemessen an der gewonnenen Sicherheit vor einem Ausspähen des Datenverkehrs relativ gering.

Nachfolgend wird die Erfindung anhand des in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert.

Die in der Zeichnung dargestellte Figur zeigt ein Blockschaltbild eines Mikrocontrollers für Sicherheitsanwendungen gemäß der Erfindung. Der Mikrocontroller umfaßt eine Anzahl von Komponenten: eine zentrale Verarbeitungseinheit (CPU) 1, die die Steuerung des Datenverkehrs abwickelt; einen Speicher 2, der Daten und abzuarbeitende Programme dauerhaft speichert; eine Peripherieeinheit 3, die Datenverkehr zu externen außerhalb des Mikrocontrollers angeordneten Schaltungen ausführt; einen Pufferspeicher 5, der Daten zwischenspeichert. Fett gezeichnete Verbindungen umfassen mehrere Leitungen.

Der nichtflüchtige Speicher 2 umfaßt eine Entschlüsselungseinrichtung 21, die eine sehr gute Verschlüsselung mit relativ langer Schlüssellänge ausführt. Die Entschlüsselung benötigt jedoch relativ lange Rechenzeit und ist schaltungstechnisch entsprechend aufwendig. Aus dem Speicher 2 auszulesende Daten werden daher im Speicher 5 zwischengepuffert, der wesentlich schneller zugriffsbereit ist. Der Speicher 5 ist ein sogenannter Cache-Speicher. Die genannten Funktionseinheiten sind untereinander über einen Bus 6 miteinander verbunden, der eine Vielzahl von Daten- und Steuerungsleitungen umfaßt.

Zwischen dem Bus 6 und jeder der Funktionseinheiten ist eine Verschlüsselungseinheit angeordnet, zum Beispiel die Einheiten 12, 32 und 52. Die Verschlüsselungseinheit verschlüsselt den von der Funktionseinheit auf den Bus 6 ausgegebenen Datenverkehr und entschlüsselt den empfangenen Datenverkehr.

Die Verschlüsselungseinheiten der Funktionseinheiten 1, 2 und 3 sind identisch ausgeführt. Beispielsweise die der CPU 1 zugeordnete Verschlüsselungseinheit 12 umfaßt ein Schlüsselregister 10, in dem ein Schlüsselwort gespeichert ist. Ein Exklusiv-ODER-Gatter 11 ist in den Datenpfad zwischen CPU 1 und Bus 6 geschaltet. Außerdem wird dem Gatter 11 auch der

Schlüssel K1 aus dem Schlüsselregister 10 zugeführt. Durch Verknüpfung des vom Bus 6 empfangenen Datenwerts mit dem Schlüsselwort K1 wird das vom Bus 6 verschlüsselt empfangene Datum T1 in Klartext T umgewandelt. Die Leitung vom Exklusiv-ODER-Gatter zur CPU 1 ist im allgemeinen nicht ohne weiteres abhörbar, da die CPU 1 eine unregelmäßige Struktur aufweist. Wenn die CPU 1 einen Datenwert T auf den Bus 6 ausgibt, wird dieser Klartextdatenwert im Exklusiv-ODER-Gatter 11 mit einem vom Schlüsselregister 10 bereitgestellten Schlüssel verknüpft und als Datenwert T1 am Bus zur Verfügung gestellt. Eine weitere Einheit, beispielsweise eine Peripheriereinheit 3, empfängt das verschlüsselte Datum T1 und entschlüsselt es auf komplementäre Weise.

Der für die Verschlüsselung in der Einheit 12 verwendete Schlüssel K1 wird taktweise verändert. Der Schlüssel wird von einem Schlüsselgenerator 61 bereitgestellt, der das Schlüsselwort zufällig erzeugt. Mit jedem von einem Taktgenerator 62 bereitgestellten Takt ändert sich das Schlüsselwort K1. Wesentlich ist, daß ein Schlüssel K1, der zur Verschlüsselung eines vor der CPU 1 ausgegebenen Datenwerts verwendet wird, ebenfalls an den anderen Verschlüsselungseinheiten zum Entschlüsseln desselben Datenwerts bereitsteht. Hierzu sind alle den jeweiligen Funktionseinheiten zugeordneten Schlüsselregister an den Zufallsgenerator 61 und Taktgenerator 62 parallel angeschlossen. Dadurch wird beispielsweise ein von der CPU 1 abgegebener Datenwert T als Datenwert T1 verschlüsselt auf den Bus ausgegeben und mit dem gleichen Schlüssel K1 an der Peripherieeinheit 3 entschlüsselt und dort als gleiches Datum T im Klartext zur Verfügung gestellt. Durch die zufallsgesteuerte Aktualisierung des Schlüssels ist eine hohe Sicherheit vor einem Entschlüsselungsversuch des über den Bus übertragenen Datums erreicht.

Dem Cache-Speicher 5 ist eine den Verschlüsselungseinrichtungen 12 und 32 entsprechende Verschlüsselungseinrichtung 52 vorgeschaltet. Die Verschlüsselungseinrichtung 52 umfaßt ein

Schlüsselregister 50, welches in gleicher Weise mit dem Taktgenerator 62 und dem Zufallsgenerator 61 verbunden ist sowie ein Exklusiv-ODER-Gatter 51, welches in den Datenpfads zwischen Bus 6 und Cache-Speicher 5 geschaltet ist. Ohne weitere Maßnahmen würde der zwischen Gatter 51 und Cache-Speicher 5 laufende Datenverkehr im Klartext vorliegen, außerdem wären die Daten im Cache-Speicher 5 im Klartext gespeichert.

Um die im Cache-Speicher 5 abgelegten Daten zusätzlich zu verschlüsseln ist eine weitere Verschlüsselungseinheit 53 vorgesehen, die mit der Verschlüsselungseinheit 52 kombiniert ist, um die von der Verschlüsselungseinrichtung 52 mittels des Schlüssels K1 entschlüsselten Daten wieder zu verschlüsseln. Die weitere Verschlüsselungseinrichtung 53 umfaßt ein Schlüsselregister 54 sowie ein Exklusiv-ODER-Gatter 55. Das Exklusiv-ODER-Gatter 55 ist zwischen das Schlüsselregister 50 und das Exklusiv-ODER-Gatter 51 geschaltet. Durch das Exklusiv-ODER-Gatter 55 werden die Schlüssel der Register 50 und 54 miteinander verknüpft. Dies bewirkt, daß der vom Exklusiv-ODER-Gatter 51 an den Cache-Speicher 5 abgegebene Datenstrom T2 verschlüsselt ist.

In entsprechender Weise werden die aus dem Cache-Speicher 5 ausgelesenen Daten T2 wieder mit dem im Schlüsselregister 54 abgelegten Schlüsselwort K2 entschlüsselt und mit dem im Schlüsselregister 50 abgelegten aktuellen veränderbaren Schlüssel K1 zur Ausgabe auf den Datenbus 6 verschlüsselt.

Solange im Cache-Speicher 5 gültige Daten gespeichert sind, die zur weiteren Verarbeitung wieder an den Bus auszulesen sind, muß das vom Schlüsselregister 54 bereitgestellte Schlüsselwort K2 unverändert gleich bleiben. Das Schlüsselwort K2 wird von einem weiteren Schlüsselgenerator 63 erzeugt. Zweckmäßigerweise wird der Schlüssel K2 geändert, wenn sich im Cache-Speicher 5 keine gültigen Daten mehr befinden. Die Aktualisierung des Schlüssels erfolgt wiederum nach einem Zufallsmuster, so daß ausreichend Sicherheit vor einer De-

chiffrierung der im Speicher gespeicherten und über den Busabschnitt zwischen Gatter 51 und Speicher 5 übertragenen Daten gewährleistet ist.

Es empfehlt sich, den Schlüssel K2 dann zu ändern, wenn der Cache-Speicher 5 nach einem Cache-Flush entleert wird. Eine solche Operation wird beispielsweise bei einem Wechsel der von der Mikroprozessoranordnung abgearbeiteten Anwendung durchgeführt. Bei einem Cache-Flush werden sämtliche Datenwerte des Cache-Speichers auf einen vorgegebenen Wert zurückgesetzt. Prinzipiell ist es auch möglich, auf ein Rücksetzen des Speicherinhalts zu verzichten, da bei einer Schlüsseländerung ohnehin der Speicherinhalt nicht mehr entschlüsselbar ist.

Durch die Erfindung wird erreicht, daß sämtlicher über den Bus 6 laufender Datenverkehr und außerdem die im Pufferspeicher zwischengespeicherten Daten stets verschlüsselt sind und nicht im Klartext vorliegen. Durch die Verwendung von Exklusiv-ODER-Gattern können symmetrische Ver- und Entschlüsselungsverfahren verwendet werden, die geringen Schaltungs- und Rechenaufwand erfordern. Die Schlüsselbreite orientiert sich an der Anzahl der Leitungen des Busses. Es können alle Leitungen oder nur ein Teil der Leitungen verschlüsselt werden. Das Schlüsselregister ist dann entsprechend kleiner. Für jede Leitung wird ein Bit eines Schlüsselwortes verwendet. Bei Busleitungen können sowohl die Datenleitungen als auch die Status- und Steuerleitungen des Busses verschlüsselt weden. Prinzipiell ist es auch möglich, einzelne sicherheitsrelevante Signalleitungen in Mikroprozessoranordnungen oder sonstigen Schaltungen unter entsprechender Anwendung der oben beschriebenen Maßnahmen zu verschlüsseln. Als Zufallsquelle für die Schlüsselgeneratoren 61 und 63 eignet sich insbesondere eine physikalische Quelle. Bei weniger Sicherheitsbedürfnis kann der Schlüssel auch durch einen Pseudo-Zufallsgenerator erzeugt werden. Die Schlüsselgeneratoren können als linear rückgekoppelte Schieberegister (LFSR) realisiert werden. Die

Aktualisierung des Schlüssels kann bei jedem Taktzyklus des Buses 6 durch den Taktgenerator 62 aktualisiert werden oder erst nach einem Ablauf einer bestimmten Anzahl von Taktzyklen. Durch geeignete Wahl der Parameter wird ein gewünschtes Maß an Sicherheit eingestellt.

Patentansprüche

1. Mikroprozessoranordnung, die umfaßt:
- eine zentrale Verarbeitungseinheit (1),
- eine weitere Einheit (2, 3, 4),
- eine Speichereinheit (5),
- einen Bus (6), über den die zentrale Verarbeitungseinheit (1), die weitere Einheit (2, 3, 4) und der Speicher (5) miteinander zum Austausch von Daten verbunden sind,
- je eine den Einheiten (1, 2, 3, 4, 5) zugeordnete erste Verschlüsselungseinheit (12, 32, 52), die zwischen den Bus (6) und der zugeordneten Einheit (1, 2, 3, 4, 5) geschaltet ist und ein Mittel (10, 50) zur Bereitstellung eines Schlüssels und ein logisches Verknüpfungselement (11, 51) umfaßt, das zwischen den Bus (6) und die zugeordnete Einheit (1, 2, 3, 5) geschaltet ist, wobei der Schlüssel für die Einheiten gleich ist und veränderbar ist,
- eine der Speichereinheit (5) zugeordnete zweite Verschlüsselungseinheit (53), die ein Mittel (54) zur Bereitstellung eines weiteren Schlüssels umfaßt sowie ein logisches Verknüpfungselement (55), das zwischen das Mittel (54) zur Bereitstellung des Schlüssels der zugeordneten ersten Verschlüsselungseinheit (50) und das logische Verknüpfungselement (51) der zugeordneten ersten Verschlüsselungseinheit (52) geschaltet ist.

2. Mikroprozessoranordnung nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t, daß
ein Generator (61) für einen Schlüssel vorgesehen ist und daß die Mittel (10, 50) zur Bereitstellung des Schlüssels der ersten Verschlüsselungseinheiten (12, 32, 52) je ein Register (10, 50) umfassen, das ausgangsseitig mit dem jeweiligen logischen Verknüpfungselement (11, 51) verbunden ist und eingangsseitig mit dem Generator (61) für den Schlüssel.

3. Mikroprozessoranordnung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Generator (61) ein Zufallsgenerator ist, durch den Binärzahlen zufallsweise erzeugbar sind.

4. Mikroprozessoranordnung nach Anspruch 3, dadurch gekennzeichnet, daß die Register (10, 50) von einem gemeinsamen Taktgenerator (62) steuerbar sind.

5. Mikroprozessoranordnung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die Mittel (54) zur Bereitstellung des zweiten Schlüssels der zweiten Verschlüsselungseinheit (53) ein Register (54) umfassen, das eingangsseitig mit einem zweiten Generator (63) für einen Schlüssel verbunden ist, und daß das logische Verknüpfungselement (55) der der zweiten Verknüpfungseinheit (53) eingangsseitig mit dem Ausgang des Registers (54) der zweiten Verschlüsselungseinheit und dem Register (50) der zugeordneten ersten Verschlüsselungseinheit (52) verbunden ist und ausgangsseitig mit einem Eingang der logischen Verknüpfungseinheit (51) der zugeordneten ersten Verknüpfungseinheit (52).

6. Mikroprozessoranordnung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die logischen Verknüpfungseinheiten (11, 51, 55) Exklusiv-ODER-Gatter sind.

7. Mikroprozessoranordnung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Speichereinheit (5) als ein flüchtiger Speicher ausgebildet ist.

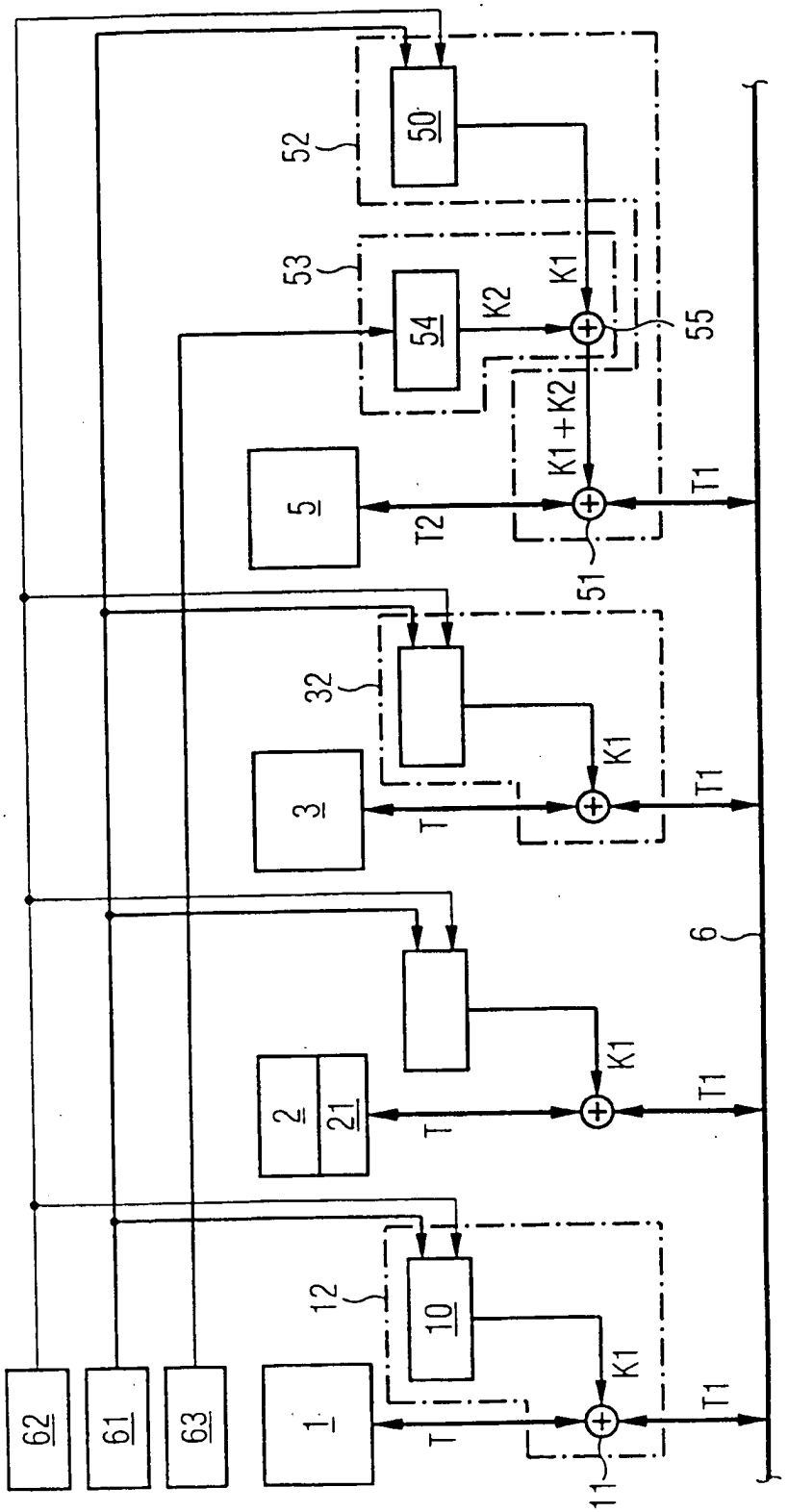
8. Mikroprozessoranordnung nach einem der Ansprüche 1 bis 7,

dadurch gekennzeichnet, daß
der zweite Generator (63) für einen Schlüssel derart steuerbar ist, daß durch ihn ein neuer Schlüssel erzeugbar ist, wenn die Speichereinheit (5) keinen gültigen Speicherinhalt aufweist.

9. Mikroprozessoranordnung nach Anspruch 8,
dadurch gekennzeichnet, daß
durch den zweiten Generator (63) der Schlüssel erzeugbar ist, nachdem die Speichereinheit (5) initialisiert worden ist.

10. Mikroprozessoranordnung nach einem der Ansprüche 1 bis 9,
dadurch gekennzeichnet, daß
ein weiterer Speicher (2) vorgesehen ist und daß die Speichereinheit (5) ein Cache-Speicher ist, in dem Daten des weiteren Speichers (2) zwischenspeicherbar sind.

1/1


50
52
53
54
K2
K1
55
K1+K2
5
T2
T1
51
32
K1
3
T
T1
6
K1
2
21
T
T1
12
10
K1
62
61
63
1
T
T1
11

INTERNATIONAL SEARCH REPORT

Intern· ·nal Application No
PCT/DE 00/04448

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G11C7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G11C G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 720 098 A (THOMSON-CSF) 3 July 1996 (1996-07-03) abstract; claims; figures page 8, line 46 -page 9, line 7	1
A	WO 99 46774 A (XILINX) 16 September 1999 (1999-09-16) abstract; claims; figures	1-3,6
A	EP 0 965 994 A (SCHLUMBERGER SYSTÈMES) 22 December 1999 (1999-12-22)	
A	GB 2 203 271 A (IBM) 12 October 1988 (1988-10-12)	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 May 2001	22/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/DE 00/04448

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0720098 A	03-07-1996	FR 2728980 A	05-07-1996
WO 9946774 A	16-09-1999	US 6118869 A	12-09-2000
EP 0965994 A	22-12-1999	FR 2779849 A	17-12-1999
		CN 1239261 A	22-12-1999
GB 2203271 A	12-10-1988	NONE	

INTERNATIONALER RECHERCHENBERICHT

Interr nales Aktenzeichen
PCT/DE 00/04448

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07F7/10 G11C7/24

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07F G11C G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
WPI Data, EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 720 098 A (THOMSON-CSF) 3. Juli 1996 (1996-07-03) Zusammenfassung; Ansprüche; Abbildungen Seite 8, Zeile 46 -Seite 9, Zeile 7	1
A	WO 99 46774 A (XILINX) 16. September 1999 (1999-09-16) Zusammenfassung; Ansprüche; Abbildungen	1-3,6
A	EP 0 965 994 A (SCHLUMBERGER SYSTÈMES) 22. Dezember 1999 (1999-12-22)	
A	GB 2 203 271 A (IBM) 12. Oktober 1988 (1988-10-12)	

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
14. Mai 2001	22/05/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichung, die zur selben Patentfamilie gehören

Intern ales Aktenzeichen
PCT/DE 00/04448

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0720098 A	03-07-1996	FR 2728980 A	05-07-1996
WO 9946774 A	16-09-1999	US 6118869 A	12-09-2000
EP 0965994 A	22-12-1999	FR 2779849 A	17-12-1999
		CN 1239261 A	22-12-1999
GB 2203271 A	12-10-1988	KEINE	